






**METHOD AND DEVICE FOR MAKING SECURE DATA ACCESS AND TRANSFERS
IN A COMPUTER SYSTEM**

Patent number: WO0105085
Publication date: 2001-01-18
Inventor: GENEVOIS CHRISTOPHE (FR); GUENEBAUD
PHILIPPE (FR)
Applicant: SCM SCHNEIDER MICROSYSTEME MIC (FR);
GENEVOIS CHRISTOPHE (FR); GUENEBAUD
PHILIPPE (FR)
Classification:
- **International:** **H04L9/32; H04L9/32;** (IPC1-7): H04L; G06F; G06K;
G07C; G07F
- **European:** H04L9/32
Application number: WO2000FR01990 20000710
Priority number(s): FR19990008908 19990709

Also published as:

 WO0105085 (A3)
 FR2796232 (A1)

Cited documents:

 XP002274300
 XP000799262
 XP000603321

Report a data error here

Abstract of WO0105085

The invention concerns a method for making secure data access and transfers in a computer system comprising at least a host and a peripheral provided with a smart card interface enabling access to the computer system while it is in use by means of smart cards. The invention also concerns a device for implementing the method. The invention is characterised in that it consists in: storing in the smart card(s) and in the host a secret key, said secret key being identical in the host and in the authorised smart cards; and during use sessions, in creating in the smart card and in the host a local session key by identical encryption of a random number using the secret key. When data are being transferred between the peripheral and the host, the method consists in: encrypting the data to be transferred by encryption means using the local session key; decrypting the transferred data symmetrically with encryption means using the other local session key; such that the transferred data are intelligible only if the same secret key is present in the host and in the smart card. The invention is applicable to a security system for authorisation and authentication.

Data supplied from the **esp@cenet** database - Worldwide

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
18 janvier 2001 (18.01.2001)

PCT

(10) Numéro de publication internationale
WO 01/05085 A2

(51) Classification internationale des brevets: H04L .
G07F /, G07C /, G06K /, G06F /

DEVELOPPEMENT ET VENTE [DE/FR]; Chez Argéo
Athélia III, Voie Atlas, F-13705 La Ciotat (FR).

(21) Numéro de la demande internationale:
PCT/FR00/01990

(72) Inventeurs; et
(75) Inventeurs/Déposants (pour US seulement):
GENEVOIS, Christophe [FR/FR]; Office Méditerranéen
de Brevets d'Invention et de Marques, Cabinet Hautier,
24, rue Massena, F-06000 Nice (FR). GUENEBAUD,
Philippe [FR/FR]; Office Méditerranéen de Brevets
d'Invention et de Marques, Cabinet Hautier, 24, rue
Masséna, F-06000 Nice (FR).

(22) Date de dépôt international: 10 juillet 2000 (10.07.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/08908 9 juillet 1999 (09.07.1999) FR

(74) Mandataire: HAUTIER, Jean-Louis; Office Méditer-
ranéen de Brevets d'Invention et de, Marques, Cabinet Hau-
tier, 24, rue Massena, F-06000 Nice (FR).

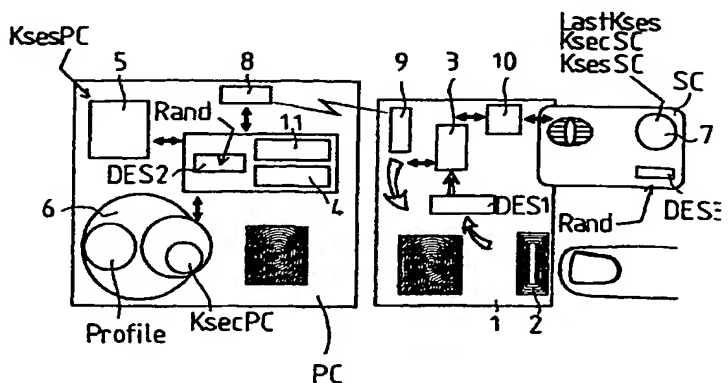
(71) Déposant (pour tous les États désignés sauf US): SCM
SCHNEIDER MICROSYSTEME MICROSYTEMES
ENTWICKLUNGS UND VERTRIERS GMBH SARL

(81) États désignés (national): AE, AL, AM, AT, AU, AZ, BA,
BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM,
EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS,

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR MAKING SECURE DATA ACCESS AND TRANSFERS IN A COMPUTER SYSTEM

(54) Titre: PROCEDE ET DISPOSITIF DE SECURISATION DE L'ACCES ET DES TRANSFERTS DE DONNEES DANS UN
SYSTEME INFORMATIQUE



(57) Abstract: The invention concerns a method for making secure data access and transfers in a computer system comprising at least a host and a peripheral provided with a smart card interface enabling access to the computer system while it is in use by means of smart cards. The invention also concerns a device for implementing the method. The invention is characterised in that it consists in: storing in the smart card(s) and in the host a secret key, said secret key being identical in the host and in the authorised smart cards; and during use sessions, in creating in the smart card and in the host a local session key by identical encryption of a random number using the secret key. When data are being transferred between the peripheral and the host, the method consists in: encrypting the data to be transferred by encryption means using the local session key; decrypting the transferred data symmetrically with encryption means using the other local session key; such that the transferred data are intelligible only if the same secret key is present in the host and in the smart card. The invention is applicable to a security system for authorisation and authentication.

[Suite sur la page suivante]

WO 01/05085 A2

Publiée:

(84) États désignés (*régional*): brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BI, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé:** La présente invention concerne un procédé de sécurisation de l'accès et des transferts de données dans un système informatique comprenant au moins un hôte et un périphérique doté d'une interface carte à puce permettant d'autoriser l'accès au système informatique lors des sessions d'utilisation par le biais de cartes à puce. Elle concerne également un dispositif apte à mettre en oeuvre le procédé. Selon l'invention, on stocke dans la ou les cartes à puce et dans l'hôte une clef secrète, ladite clef secrète étant identique dans l'hôte et dans les cartes à puce autorisées; et, lors des sessions d'utilisation, on crée dans la carte à puce et dans l'hôte une clef de session locale par chiffrement identique d'un même nombre aléatoire en utilisant la clef secrète; Lors des transferts de données entre le périphérique et l'hôte : on crypte les données à transférer par des moyens de chiffrement utilisant la clef de session locale on décrypte les données transférées de façon symétrique par des moyens de chiffrement utilisant l'autre clef de session locale; de sorte que les données transférées ne soient intelligibles que si la même clef secrète est présente dans l'hôte et dans la carte à puce. Application au système de sécurisation d'autorisation et d'authentification.

5

10

15 « Procédé et dispositif de sécurisation de l'accès et des transferts de données dans un système informatique »

20

25 La présente invention concerne tout d'abord un procédé de sécurisation de l'accès et des transferts de données dans un système informatique. Elle concerne ensuite un dispositif apte à mettre en œuvre le procédé.

30 Le dispositif, intégré dans le système informatique, comprend au moins un hôte et un périphérique doté d'une interface carte à puce permettant d'autoriser l'accès au système informatique lors des sessions d'utilisation par le biais de cartes à puce.

L'invention s'appliquera aux systèmes de sécurisation, d'autorisation et d'authentification. Particulièrement, l'authentification par carte à puce et capteurs biométriques est visés.

5 On entend par carte à puce un support d'autorisation comprenant un code ou une clé d'authentification du porteur. Le lecteur de carte à puce utilisable pourra notamment être conforme aux normes PCMCIA.

10 On entend par système informatique toute installation comportant notamment un serveur ou un ou plusieurs ordinateurs vis à vis de laquelle un accès ou une communication est possible. De nombreux systèmes informatiques sont visés par l'invention qui peut notamment concerner les systèmes où un secret est nécessaire pour toute accès ou certains accès
15 suivant le degré de sécurisation.

Dans ce domaine, on connaît le document W08203286 qui concerne un support de données se présentant de préférence sous la forme d'une carte personnelle contenant des informations concernant le titulaire, la société d'émission de
20 la carte, le numéro de compte, etc..., et destiné à une utilisation manuelle à l'endroit d'utilisation ou à l'aide d'un dispositif d'entrée en mémoire/de sortie de la mémoire inclus dans un équipement d'un terminal. Ce support de donnée comprend des moyens de traitement interne des informations
25 d'identification fournies concernant le titulaire pendant un processus de vérification et de génération d'un signal d'acceptation résultant de la vérification de l'identité et/ou du droit du titulaire à utiliser le support de données. Dans ces moyens, un dispositif de vérification est prévu pour
30 effectuer ce processus de vérification et comprend un dispositif détecteur pour détecter l'extrémité d'un doigt du titulaire et obtenir l'information de lignes papillaires.

De telles techniques font le plus souvent appel à des

dispositifs unitaires complexes où tous les éléments sont intégrés afin d'éviter les transferts d'information entre différents composants distincts. Par conséquent, ces dispositifs sont coûteux et de conception complexe.

5 On connaît par ailleurs du document W09908238 un assistant numérique personnel client portable pourvu d'un écran tactile ou d'une autre interface utilisateur équivalente. Cet assistant numérique personnel comporte un microphone et une UC locale permettant de traiter les
10 commandes vocales ainsi que des données biométriques d'authentification de l'utilisateur.

Une autorisation biométrique est proposée selon de telles techniques mais, cependant, elle n'évite pas tous risques de fraude. Par exemple, dans certains cas, le doigt ou la carte
15 peuvent être simulés ou le périphérique d'authentification peut être substitué par un autre périphérique fournissant des signaux équivalents. Dans ce cas, l'analyse des signaux de communication permet de déduire les clés du protocole ou les messages. Cela permet à une tierce personne non autorisée
20 d'effectuer un rejeu du scénario d'authentification pour duper le système et accéder à des ressources ou des données qui devraient être tenues secrètes.

L'invention a pour but de remédier aux inconvénients des techniques actuelles. Elle permet une sécurisation totale dans
25 les transferts de données ou dans les autorisations d'accès à un système informatique. Elle permet d'effectuer une authentification par le biais d'un périphérique, le périphérique étant capable de communiquer avec un système hôte sans pour autant risquer, lors du transfert, une soustraction
30 des données.

L'un des avantages de l'invention est que les clés secrètes utilisées pour le chiffrement des données ne sont jamais utilisables directement. De plus, ces clés secrètes ne

sont jamais transférées entre deux éléments constitutifs du système informatique même de façon codée.

Ainsi, aucune information fondamentale permettant de contourner les conditions d'autorisation ne peut être
5 transférée en milieu hostile.

Dans le cadre de l'utilisation d'un capteur biométrique, l'invention permet une authentification conditionnée à la présence de la carte à puce qui a réalisé la dernière autorisation d'accès. De cette façon, trois conditions sont
10 cumulées à savoir la reconnaissance de la mesure biométrique, la reconnaissance de la carte à puce dans la session actuelle et la reconnaissance de la carte à puce en tant que dernière carte à puce utilisée pour la dernière autorisation.

L'invention réalise ainsi une parfaite sécurisation sans
15 pour autant nécessiter la mise en œuvre de moyens particulièrement complexes.

La présente invention concerne un procédé de sécurisation de l'accès et des transferts de données dans un système informatique comprenant au moins un hôte et un
20 périphérique doté d'une interface carte à puce permettant d'autoriser l'accès au système informatique lors des sessions d'utilisation par le biais de cartes à puce,

caractérisé par le fait qu'on stocke dans la ou les cartes à puce et dans l'hôte une clef secrète, ladite clef
25 secrète étant identique dans l'hôte et dans les cartes à puce autorisées ;

et que, lors des sessions d'utilisation, on crée dans la carte à puce et dans l'hôte une clef de session locale par chiffage identique d'un même nombre aléatoire en utilisant la
30 clef secrète ;

et que lors des transferts de données entre le périphérique et l'hôte :

- on crypte les données à transférer par des moyens de

chifffrage utilisant la clef de session locale

- on décrypte les données transférées de façon symétrique par des moyens de chifffrage utilisant l'autre clef de session locale ;

5 de sorte que les données transférées ne soient intelligibles que si la même clef secrète est présente dans l'hôte et dans la carte à puce.

Le procédé pourra se présenter sous les modes de réalisation énoncés ci-après :

10 - le nombre aléatoire est généré au sein de l'hôte et transmis en clair à la carte à puce.

- on dote le périphérique d'au moins un capteur biométrique.

Au cours de la cession :

15 - on mémorise de façon non volatile la clef de session dans la carte à puce pour sa réutilisation à la session suivante comme clef de session précédente

- on crypte, puis on mémorise dans l'hôte le profil biométrique authentique à comparer avec la mesure du capteur biométrique, par le biais des moyens de chifffrage utilisant la clef de session locale,
20 afin que la même carte à puce, comportant la clef de session précédente, soit nécessaire pour le décryptage du profil authentique lors de la session suivante.

25 - on crypte les mesures du capteur biométrique au sein du périphérique avant tout transfert vers l'hôte, par le biais de moyens de chifffrage en utilisant la clé de session locale.

- on constitue le profil biométrique authentique par :

- mesure par le capteur biométrique ;

30 - cryptage au sein du périphérique ;

- transfert à l'hôte,

- décryptage au sein de l'hôte par le biais de moyens de chifffrage en utilisant la clé de session locale ;

- traitement des données de mesure ;
- cryptage au sein de l'hôte par le biais des moyens de chiffrage en utilisant la clé de session locale
- mémorisation dans un fichier en mémoire volatile.

5 - On effectue les étapes suivantes pour
l'authentification :

- mesure par le capteur biométrique ;
- cryptage au sein du périphérique ;
- transfert à l'hôte;
- 10 - décryptage au sein de l'hôte par le biais de moyens de cryptage en utilisant la clef de session local ;
- traitement des données de mesure ;
- comparaison entre les données de mesure traitées et le profil biométrique mémorisé.

15 L'invention concerne également un dispositif de sécurisation de l'accès et des transferts de données dans un système informatique, comprenant au moins un hôte et un périphérique doté d'une interface carte à puce permettant d'autoriser l'accès au système informatique lors des
20 sessions d'utilisation par le biais de cartes à puce, apte à mettre en œuvre le procédé caractérisé par le fait qu'il comporte

- des moyens de mémorisation non volatile pour le stockage d'une clef secrète identique dans les cartes à puce
25 autorisées et l'hôte,

- des moyens générateurs d'un nombre aléatoire lors des sessions d'utilisation, ledit nombre aléatoire étant exploitable par l'hôte et la carte à puce,

- des moyens de chiffrage identiques dans la carte à
30 puce, le périphérique et l'hôte pour la création dans la carte à puce et l'hôte d'une clef de session locale par chiffrage du nombre aléatoire en utilisant la clef secrète et le cryptage de toute donnée puis son décryptage, lors des transferts entre

le périphérique et l'hôte en utilisant la clef de session locale, de sorte que les données transférées ne sont intelligibles que si la même clef secrète est présente dans l'hôte et dans la carte à puce.

5 Le dispositif pourra se présenter sous les modes de réalisation énoncés ci après :

- les moyens générateurs d'un nombre aléatoire sont intégrés à l'hôte.

- l'hôte comprend une mémoire volatile permettant le
10 stockage temporaire de la clef de session locale.

- la liaison entre l'hôte et le périphérique est réalisée par un bus universel série reliant un port de l'hôte à un port du périphérique.

- les moyens de chiffage sont formés par des modules
15 mettant en œuvre un algorithme de chiffage.

- le périphérique est doté d'au moins un capteur biométrique.

- le profil biométrique authentique à comparer avec la mesure du capteur biométrique est stocké dans la mémoire non
20 volatile de l'hôte dans un fichier après son cryptage par les moyens de chiffage.

- l'hôte comprend des moyens de traitement des mesures du capteur biométrique et des moyens de comparaison desdits mesures et du fichier.

25 Les dessins ci-joints sont donnés à titre d'exemple indicatif et non limitatif. Ils représentent un mode de réalisation selon l'invention. Ils permettront de la comprendre aisément.

La figure 1 est une vue générale du dispositif selon
30 l'invention dans un mode de réalisation particulier

La figure 2 est un diagramme mettant en évidence des étapes de mise en œuvre du procédé de l'invention.

La présente invention s'adresse à des systèmes

informatiques qui comprendront au moins un hôte (PC) et un périphérique (1).

Des applications très diverses telles que l'accès et la modification de bases de données ou encore des passages d'ordres bancaires sont dans le champ de l'invention.

L'hôte (PC) pourra ainsi être un ordinateur ou un serveur informatique. Il comprendra les organes nécessaires à l'application envisagée et pour le moins un processeur et un espace mémoire.

Pour procéder aux autorisations d'accès, un périphérique (1) est également présent. Il comprend une interface carte à puce (10) pour la liaison (lecture - écriture) avec une ou plusieurs cartes à puce (SC).

Cette configuration est illustrée en figure 1.

L'interface carte à puce (10) pourra être du type PCMCIA. Cependant, d'autres formats sont utilisables.

De préférence, l'interface (10) est intégrée dans le périphérique (1) pour sécuriser leurs communications. Par ailleurs la carte à puce (SC), elle-même, peut être intégrée de façon à constituer un périphérique (1) autonome pour lequel la carte à puce (SC) est non amovible et, par exemple, montée en usine.

Selon l'invention, le dispositif comportent des moyens de mémorisation (6,7) dans l'hôte (PC), et dans la carte à puce (SC). Une mémoire du type EEPROM peut-être affectée à cet effet.

Les moyens de mémorisation (6,7) permettent le stockage d'une clé secrète, par nature connue en soi, dans l'hôte (PC) et dans la carte à puce (SC).

On attribue la référence Ksec SC à la clé secrète stockée dans la carte à puce (SC) et la référence Ksec PC à celle stockée dans l'hôte (PC).

Selon l'invention, les clés secrètes Ksec PC et Ksec SC

sont identiques si la carte à puce (SC) est une carte autorisée. Comme explicité plus loin, cette identité de clé sera nécessaire à l'autorisation.

Le dispositif comporte en outre des moyens générateurs
5 (11) d'un nombre aléatoire (Rand). Dans le cas préférentiel illustré en figure 1, les moyens générateurs (11) sont intégrés à l'hôte (PC).

Un nombre aléatoire (Rand) sera généré à chaque session d'utilisation où le dispositif d'autorisation sera appelé à
10 fonctionner.

Le nombre aléatoire (Rand) généré est exploité à la fois par l'hôte (PC) et par la carte à puce (SC) à laquelle il peut être transmis en clair.

Pour exploiter le nombre aléatoire (Rand), des moyens de
15 chiffrage (DES 2,3) sont présents dans l'hôte (PC) et la carte à puce (SC). Ils seront constitués de façon identique.

Ils assurent le chiffrage du nombre aléatoire (Rand) en utilisant la clé secrète (Ksec SC, Ksec PC).

De cette façon, on obtient deux clefs de session
20 locale (Kses SC, Kses PC) qui ne seront identiques que si les clefs secrètes (Ksec SC, Ksec PC) sont identiques.

Dans l'hôte (PC) une mémoire volatile (5) telle la RAM (Random Access Memory) d'un ordinateur stockera la clef de session locale (Kses PC). Ce stockage sera donc temporaire,
25 pour assurer une plus grande sécurité et éviter toute récupération de la clef hors de la session en cours.

Dans la carte à puce (SC), la clef de session locale (Kses SC) pourra être stockée en mémoire non volatile (7).

De cette façon, il sera possible de l'utiliser en tant
30 que clef de session précédente (Last Kses) à la session suivante et de l'employer comme autre condition d'accès : il faudra alors posséder non seulement la bonne clef secrète (Ksec SC) mais aussi la bonne clef de session précédente (Last

Kses).

Les moyens de chiffrage (DES 2, DES 3) pourront être de conception courante et particulièrement se présenter sous forme de modules mettant en œuvre un algorithme de chiffrage.

5 Le périphérique comportera également des moyens de chiffrage (DES 1).

Dans un mode de réalisation préféré, ces derniers moyens de chiffrage (DES 1) sont semblables aux autres moyens de chiffrage (DES 2, DES 3). De cette façon, on exploite le même
10 système de codage -décodage pour chiffrer le nombre aléatoire (Rand) et pour crypter les données à transférer.

En effet, les moyens de chiffrage (DES 1, DES 2) présents dans le périphérique (1) et l'hôte (PC) permettent le cryptage de toute donnée avant son transfert puis son décryptage après
15 le transfert.

Dans le cas où l'interface carte à puce (10) est externe au périphérique (1), les moyens de chiffrage (DES 3) pourront aussi avoir cette fonction de cryptage de données pour les transferts vers le périphérique (1) ou l'hôte (PC).

20 Les moyens de chiffrage (DES1) peuvent être intégrés directement dans le capteur biométrique (2).

Pour le cryptage ou le décryptage symétrique des données, c'est la clef de session locale (Kses PC, Kses SC) qui est utilisée.

25 Ainsi, les éléments constitutifs du système informatique ne pourront se comprendre que si les clefs de session locale (Kses PC, Kses SC) sont identiques, sans pour autant que des codes secrets ou des clefs secrètes soient transférés.

Aucune tentative de récupération de ces clefs sur les
30 voies de transfert ne pourra aboutir.

Dans un mode de réalisation, la liaison entre le périphérique (1) et l'hôte (PC) s'effectue par un bus universel série, souvent dénommé USB.

La voie de transmission de données sera exploitée dans ce bus. La voie d'alimentation électrique pourra l'être également, par exemple pour l'alimentation totale ou partiel du périphérique (1).

5 Dans un mode préféré de réalisation, correspondant à l'illustration des figures 1 et 2, le périphérique (1) est doté d'au moins un capteur biométrique (2). A titre d'exemple non limitatif, un capteur de saisie d'empreinte digitale peut être utilisé.

10 La mesure du capteur biométrique (2) sera comparée avec un profil biométrique authentique préalablement mémorisé en mémoire non volatile (6) de l'hôte (PC).

Pour sécuriser le stockage du profil, celui-ci est crypté avant mémorisation par le biais des moyens de chiffrage (DES
15 2) en utilisant la clef de session (Kses PC).

Le fichier obtenu est dénommé profile sur la figure 1.

Pour effectuer la comparaison entre le profil authentique et la mesure du capteur biométrique (2), des moyens de traitement (4) des mesures et des moyens de comparaison seront
20 utilisés.

Par exemple, dans le cas de mesure d'empreintes digitales, le traitement pourra consister en un traitement d'image et une extraction des minuties.

Le fichier Profile pourra être un fichier de minuties,
25 dans ce cas précis.

Les figures 1 et 2 montrent en illustration de l'empreinte digitale avec un trait plus foncé pour la mesure issue du capteur (2) et en trait plus clair pour les données après extraction des minuties.

30 Le fonctionnement du dispositif et les étapes du procédé sont présentés ci-après dans un mode de réalisation conforme aux figures et particulièrement à la figure 2.

Pour la création du fichier Profile, une mesure du

capteur biométrique (2) est effectuée au niveau du périphérique (1).

Avant transfert, ces données sont cryptées par les moyens de chiffrage (DES 1). Le cryptage est possible par la
5 génération du nombre aléatoire (Rand) au sein de l'hôte (PC) et la création consécutive des clefs de session locales (Kses SC, Kses PC). Comme décrit précédemment, l'emploi d'une carte à puce comportant la clef secrète requise (Ksec SC) conditionnera, préalablement, le bon déroulement de cette
10 opération.

Après cryptage, les données de mesure sont transférées vers l'hôte (PC) depuis le port (9) du périphérique (1) vers le port (8) de l'hôte (PC).

Pour traitement, les données sont d'abord décryptées par
15 une opération symétrique à la précédente au moyen des moyens de chiffrage (DES 2) avec la clef de session locale (Kses PC).

Si les clefs de session locales ne sont pas identiques, le décryptage n'a pas l'effet escompté.

Dans le cas illustré en figure 2, les moyens de
20 traitement (4) permettent le traitement d'image et l'extraction des minuties.

Après cryptage par la clef (Kses PC), un fichier Profile est créé avec les données sur la mémoire non volatile (6).

Lors d'une session où l'accès doit être sécurisé, une
25 autorisation est déjà réalisée par la carte à puce (SC) qui doit comporter le bon code secret.

Comme expliqué plus loin, la carte à puce (SC) participera aussi à l'autorisation faite par l'authentification biométrique.

30 Cette authentification comprend d'abord la mesure des données biométriques de la personne utilisatrice. Son empreinte digitale est saisie dans le cas illustré.

Comme pour la saisie du profil authentique, un cryptage

avant transfert puis un décryptage sont réalisés en utilisant les clefs de session locales (Kses SC, Kses PC). Le traitement nécessaire des données est alors réalisé.

5 Dans le cas préféré où le profil authentique a été crypté avant mémorisation dans l'hôte (PC), la comparaison ne pourra aboutir que si le profil authentique peut être correctement décrypté auparavant.

10 Pour ce faire, l'utilisateur devra en plus fournir à l'hôte (PC) la clef de session précédente (Last Kses) par laquelle le cryptage du profil authentique a été effectué. Cette fourniture ne sera possible que par usage de la même carte à puce (SC) ayant servi à la session précédente et sur laquelle, dans ce mode de réalisation, la clef de session (Last Kses) précédente a été stockée.

15 Bien entendu, le Profil authentique peut aussi être stocké non crypté pour ne pas nécessiter cette condition d'accès supplémentaire.

20 Il peut par ailleurs être stocké, non dans l'hôte (PC) mais sur la carte à puce (SC) qui sera donc obligatoirement réutilisée à la session suivante. Son transfert vers la carte à puce (SC) utilisera le cryptage décryptage décrit précédemment. Le fichier profile sera transféré vers l'hôte (PC) en même temps que les données de mesure pour procéder à la comparaison.

25 Après comparaison, l'accès au système sera autorisé ou non.

Le même principe de cryptage pourra être employé pour les transferts de toute donnée en cours de session.

REFERENCES

- PC - hôte
SC - Carte à puce
Rand - nombre aléatoire
- 5 Ksec PC - clef secrète de l'hôte
Ksec SC - clef secrète de la carte à puce
Kses PC - clef de session locale de l'hôte
Kses SC - clef de session locale de la carte à puce
Last Kses - clef de session précédente
- 10 DES 1 - moyen de chiffage du périphérique
DES 2 - moyen de chiffage de l'hôte
DES 3 - moyen de chiffage de la carte à puce
Profile - fichier
- 15 1. Périphérique
2. Capteur biométrique
3. Microcontrôleur
4. Moyens de traitement
5. Mémoire volatile
- 20 6. Mémoire non volatile de l'hôte
7. Mémoire non volatile de la carte à puce
8. Port de l'hôte
9. Port du périphérique
10. Interface carte à puce
- 25 11. Moyens générateurs.

REVENDICATIONS

1. Procédé de sécurisation de l'accès et des transferts de données dans un système informatique comprenant au moins un
5 hôte (PC) et un périphérique (1) doté d'une interface carte à puce (10) permettant d'autoriser l'accès au système informatique lors des sessions d'utilisation par le biais de cartes à puce (SC),

caractérisé par le fait qu'on stocke dans la ou les
10 cartes à puce (SC) et dans l'hôte (PC) une clef secrète (Ksec SC, Ksec PC), ladite clef secrète étant identique dans l'hôte (PC) et dans la ou les cartes à puce (SC) autorisées ;

et que, lors des sessions d'utilisation, on crée dans la carte à puce (SC) et dans l'hôte (PC) une clef de session
15 locale (Kses PC, Kses SC) par chiffage identique d'un même nombre aléatoire (Rand) en utilisant la clef secrète (Ksec PC, Ksec SC) ;

et que lors des transferts de données entre le périphérique (1) et l'hôte (PC) :

20 - on crypte les données à transférer par des moyens de chiffage (DES 1, DES 2) utilisant la clef de session locale (Kses PC, Kses SC)

- on décrypte les données transférées de façon symétrique par les moyens de chiffage (DES 1, DES 2) utilisant l'autre
25 clef de session locale (Kses SC, Kses PC) ;

de sorte que les données transférées ne soient intelligibles que si la même clef secrète (Ksec PC, Ksec SC) est présente dans l'hôte (PC) et dans la carte à puce (SC).

2. Procédé selon la revendication 1,
30 caractérisé par le fait que le nombre aléatoire (Rand) est généré au sein de l'hôte (PC) et transmis en clair à la carte à puce (SC).

3. Procédé selon l'une des revendications 1 ou 2,

caractérisé par le fait qu'on dote le périphérique (1) d'au moins un capteur biométrique (2).

4. Procédé selon la revendication 3,

caractérisé par le fait qu'au cours de la session :

5 - on mémorise de façon non volatile la clef de session (Kses SC) dans la carte à puce (SC) pour sa réutilisation à la session suivante comme clef de session précédente (Last Kses)

- on crypte, puis on mémorise dans l'hôte (PC) ou dans la carte à puce (SC) le profil biométrique authentique à comparer
10 avec la mesure du capteur biométrique (2), par le biais des moyens de chiffrage (DES 2) utilisant la clef de session locale (Kses PC),

afin que la même carte à puce (SC), comportant la clef de session précédente (Last Kses), soit nécessaire pour le
15 décryptage du profil authentique lors de la session suivante.

5. Procédé selon l'une des revendications 3 ou 4,

caractérisé par le fait qu'on crypte les mesures du capteur biométrique (2) au sein du périphérique (1) avant tout transfert vers l'hôte (PC), par le biais de moyens de
20 chiffrage (DES 1) en utilisant la clé de session locale (Kses SC).

6. Procédé selon la revendication 5,

caractérisé par le fait qu'on constitue le profil biométrique authentique par :

25 - mesure par le capteur biométrique (2) ;

- cryptage au sein du périphérique (1) ;

- transfert à l'hôte (PC),

- décryptage au sein de l'hôte (PC) par le biais de moyens de chiffrage (DES2) en utilisant la clé de session
30 locale (Kses PC) ;

- traitement des données de mesure ;

- cryptage au sein de l'hôte (PC) par le biais des moyens de chiffrage (DES2) en utilisant la clé de session locale

(Kses PC)

- mémorisation dans un fichier (Profile) en mémoire non volatile.

7. Procédé selon les revendications 5 et 6,
5 caractérisé par le fait qu'on effectue les étapes suivantes pour l'authentification :

- mesure par le capteur biométrique (2);

- cryptage au sein du périphérique (1) ;

- transfert à l'hôte (PC) ;

10 - décryptage au sein de l'hôte (PC) par le biais de moyens de cryptage (DES 2) en utilisant la clef de session locale (Kses PC) ;

- traitement des données de mesure ;

15 - comparaison entre les données de mesure traitées et le profil biométrique mémorisé.

8. Dispositif de sécurisation de l'accès et des transferts de données dans un système informatique comprenant au moins un hôte (PC) et un périphérique (1) doté d'une interface carte à puce (10) permettant d'autoriser l'accès au
20 système informatique lors des sessions d'utilisation par le biais de cartes à puce (SC), apte à mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 7,

caractérisé par le fait qu'il comporte :

25 - des moyens de mémorisation non volatiles (6,7) pour le stockage d'une clef secrète (Ksec SC, Ksec PC) identique dans les cartes à puce (SC) autorisées et l'hôte (PC),

- des moyens générateurs (11) d'un nombre aléatoire (Rand) lors des sessions d'utilisation, ledit nombre aléatoire étant exploitable par l'hôte (PC) et la carte à puce (SC),

30 - des moyens de chiffage (DES 1, 2, 3) identiques dans la carte à puce (SC), le périphérique (1) et l'hôte (PC) pour la création dans la carte à puce (SC) et l'hôte (PC) d'une clef de session locale (Kses SC, Kses PC) par chiffage du

nombre aléatoire (Rand) en utilisant la clef secrète (Ksec SC, Ksec PC) et le cryptage de toute donnée puis son décryptage, lors des transferts entre le périphérique (1) et l'hôte (PC) en utilisant la clef de session locale (Kses SC, Kses PC),

5 de sorte que les données transférées ne sont intelligibles que si la même clef secrète (Ksec PC, Ksec SC) est présente dans l'hôte (PC) et dans la carte à puce (SC).

9. Dispositif selon la revendication 8,

caractérisé par le fait que les moyens générateurs (11)
10 d'un nombre aléatoire (Rand) sont intégrés à l'hôte (PC).

10. Dispositif selon l'une quelconque des revendications 8 ou 9,

caractérisé par le fait que l'hôte (PC) comprend une mémoire volatile (5) permettant le stockage temporaire de la
15 clef de session locale (Kses PC).

11. Dispositif selon l'une quelconque des revendications 8 à 10,

caractérisé par le fait que la liaison entre l'hôte (PC) et le périphérique (1) est réalisée par un bus universel série
20 reliant un port (8) de l'hôte (PC) à un port (9) du périphérique (1).

12. Dispositif selon l'une quelconque des revendications 8 à 11,

caractérisé par le fait que les moyens de chiffrage (DES
25 1, 2, 3) sont formés par des modules mettant en œuvre un algorithme de chiffage.

13. Dispositif selon l'une quelconque des revendications 8 à 12,

caractérisé par le fait que le périphérique (1) est doté
30 d'au moins un capteur biométrique (2).

14. Dispositif selon la revendication 13,

caractérisé par le fait que le profil biométrique authentique à comparer avec la mesure du capteur biométrique

(2) est stocké dans la mémoire non volatile (6) de l'hôte (PC) dans un fichier (Profile) après son cryptage par les moyens de chiffrage (DES 2).

15. Dispositif selon la revendication 14,
5 caractérisé par le fait que l'hôte (PC) comprend des moyens de traitement (4) des mesures du capteur biométrique (2) et des moyens de comparaison desdites mesures et du fichier (Profile).

